

Notice of Allowability	Application No.	Applicant(s)	
	09/938,790	ALTEN, ALEXANDER I.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to The Request for Continued Examination and amendment received 21 September 2006.
2. ☒ The allowed claim(s) is/are 13-23.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. <input type="checkbox"/> Notice of References Cited (PTO-892) 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Notice of Informal Patent Application 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 9. <input type="checkbox"/> Other _____ |
|---|---|


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 21 September 2006 has been entered.
2. By the above response, Claims 13 and 19 have been amended. No claims have been added or canceled. Claims 13-23 are currently pending in the present application.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Richard Butler on 06 November 2006. As discussed with Mr. Butler, the

amendments are made to avoid issues of insufficient written description under 35 U.S.C. 112, first paragraph.

4. The application has been amended as follows:

IN THE TITLE:

Please **CHANGE THE TITLE** to:

System and Methods for a Vernam Stream Cipher

IN THE CLAIMS:

Please **REPLACE Claims 13 and 19** with the following amended claims:

13. A method for enciphering a sequence of clear text data values comprising:
- a. nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets wherein each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value and wherein the plurality of mixing keys are random and secret;
 - b. performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads ~~wherein the plurality of~~

- ~~large random pads have less entropy than the plurality of shuffled large random secrets;~~
- c. circularly rotating the values of each of the plurality of large random pads according to a plurality of random rotation values thus forming a plurality of rotated large random pads wherein the plurality of random rotation values are random and secret;
 - d. randomly shuffling a portion of each of the plurality of rotated large random pads according to a plurality of working keys thus forming a plurality of randomly rotated and randomly shuffled large random pads wherein the plurality of working keys are random and secret;
 - e. performing an exclusive OR function on the plurality of randomly rotated and randomly shuffled large random pads to produce a final pad ~~wherein the final pad has less entropy than the plurality of randomly rotated and randomly shuffled large random pads;~~
 - f. selecting a portion of the final pad to form a finite key stream; and
 - g. performing an exclusive OR function with the finite key stream with the sequence of clear text data values.
19. A method for deciphering a sequence of cipher text data values comprising:
- a. nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets wherein each of the plurality of large random secrets is a random

- value and further wherein the plurality of shuffled large random secrets are each a random value and wherein the plurality of mixing keys are random and secret;
- b. performing an exclusive OR on the plurality of shuffled large random secrets to produce a plurality of large random pads ~~wherein the plurality of large random pads have less entropy than the plurality of shuffled large random secrets~~;
 - c. circularly rotating the values of each of the plurality of large random pads according to a plurality of random rotation values thus forming a plurality of rotated large random pads wherein the plurality of random rotation values are random and secret;
 - d. randomly shuffling a portion of each of the plurality of rotated large random pads according to a plurality of working keys thus forming a plurality of randomly rotated and randomly shuffled large random pads wherein the plurality of working keys are random and secret;
 - e. performing an exclusive OR function on the plurality of randomly rotated and randomly shuffled large random pads to produce a final pad ~~wherein the final pad has less entropy than the plurality of randomly rotated and randomly shuffled large random pads~~;
 - f. selecting a portion of the final pad to form a finite key stream; and
 - g. performing an exclusive OR function with the finite key stream with the sequence of cipher text data values.

Allowable Subject Matter

5. Claims 13-23 are allowed.

6. The following is an examiner's statement of reasons for allowance:

Independent Claim 13 is directed to a method for stream cipher encryption, and independent Claim 19 is directed to a corresponding method for decryption. The use of stream cipher encryption is generally well known. Further, the cited prior art, notably Koopman, Jr., US Patent 5696828, and Wilson et al, US Patent 5295188, generally disclose several of the claimed features. In particular, the cited art discloses several steps, such as nested shuffling, rotation, shuffling, and XOR operations, to be used to generate keys from source bits for use with a Vernam stream cipher. However, none of the cited art, neither Koopman nor Wilson nor the other cited art, such as Ritter, US Patent 5623549, and Schneier, *Applied Cryptography*, discloses the specifically claimed sequence of steps for generating keys to be used in encryption or decryption by stream ciphers. Therefore, the claims are allowable over the cited prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

240
zad